IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Dwork	)	Art Unit: 2135
Serial No.: 09/487,502	)	Examiner: Seal
Filed: January 19, 2000	)	**AM9-99-0138**
For: **DIGITAL SIGNATURE SYSTEM AND METHOD BASED ON HARD LATTICE PROBLEM**	)	June 7, 2004 750 B STREET, Suite 3120 San Diego, CA 92101

APPEAL BRIEF

This appeal brief is submitted under 35 U.S.C. §134. This appeal is further to Appellant's Notice of Appeal filed herewith.

Table of Contents

(1) Real Party in Interest

The real party in interest is IBM Corp.

(2) Related Appeals/Interferences

No other appeals or interferences exist which relate to the present application or appeal.

(3) Status of Claims

Claims 1-35 are pending and finally rejected.

(4) Status of Amendments

No amendments are outstanding.

(5) Summary of Invention

Claim 1 recites a computer-implemented method for digitally signing data that includes generating a lattice $\mathcal{L}$ which has at least one short basis establishing a private key and at least one long basis establishing a public key. The method further includes mapping the message μ or a concatenation thereof to a message point "x" in n-dimensional space using a function "f" that renders infeasible the possibility of mapping two messages together in the space. The method also includes finding a lattice point "y" of the lattice $\mathcal{L}$ that is close to the message point "x" using the short basis.

Instead of reciting the result of Claim 1 (mapping the message μ or a concatenation thereof to a message point "x" in a way that renders infeasible the possibility of mapping two messages together in the space), Claim 12 sets forth a specific modality for doing so, specifically by mapping the message μ or a concatenation thereof to a message point "x" in n-dimensional space wherein "x" is a point of a grid or a point of an auxiliary lattice, and then finding a point "y" of a key lattice $\mathcal{L}$ that is not the same as the auxiliary lattice.

(6) Issues

(a) Whether Claims 1-11 and 26-35 are unpatentable under 35 U.S.C. §112 as being indefinite.

(b) Whether Claims 1-11 and 19-25 are unpatentable under 35 U.S.C. §103 as being obvious over Atjai/Dwork in view of Diffie-Hellman.

(c) Whether Claims 12-18 and 26-35 are unpatentable under 35 U.S.C. §103 as being obvious over Atjai/Dwork in view of Diffie-Hellman.

(7) Grouping of Claims

Independent Claims 1 and 19 recite a patentably distinct result - rendering infeasible the mapping of two messages close together in space - whereas independent Claims 12 and 26 recite specific modalities for achieving that result, namely, using an auxiliary lattice or grid (Claim 12) or set of spaced-apart points (Claim 26). Neither of these patentable features has been shown in the prior art but more to the point the modality claims have been conflated with the result claims. Accordingly, considering Claims 1 and 19 separately from Claims 12 and 26 is necessary to avoid underdeveloped examination.

(8a) Argument

The indefiniteness rejections stem from the allegation that it is unclear what is meant by "rendering infeasible the possibility of mapping two messages together in space". A rhetorical question is asked about "sticking two letters in the same envelope", without ever explaining why the skilled artisan would find the meaning of the claims unclear when read in light of the specification, MPEP §2173. Diligent compliance with the MPEP could have prevented this rejection, see, e.g., bottom of page 8, last line and ensuing discussion. Indeed, the examiner himself has figured out that when read in light of the specification, one way (albeit perhaps not the only way) to read the claims is to regard them as stating that two points fall either

inside or outside a predetermined distance, contradicting his own allegation of indefiniteness. Simply because the claims contain a broad recitation does not render them indefinite, MPEP §2173.04 ("breadth is not indefiniteness"). It is respectfully requested that this rejection be reversed.

(8b) Argument

Appellant will bring some laser-like focus to bear on the deficiency of the present rejection of Claims 1 and 19. Both these claims recognize that in a digital signature scheme using lattices, it is important to render infeasible the possibility of mapping two messages together in the space. The rejection alleges that this is taught in the present inventor's previous work, Atjai/Dwork, at page 4, first complete paragraph from the top. This section of Atjai/Dwork states in its entirety:

> "In all three cryptosystems the value one is encrypted by choosing a random point in a particular region in R^n (the exact depends on the scheme)."

Thus, contrary to the allegation in the rejection, this section of Atjai/Dwork does not discuss mapping and it does not even discuss more than a single point, much less the necessity of using a predetermined distance for accepting or rejecting two points as alleged. The allegation, predicated as it is on a non-existent teaching, is legally insufficient to support the rejection, which consequently must be reversed.

Appellant has not only pointed this out but has also observed that Diffie-Hellman nowhere mentions lattices, so it cannot be used to supply the missing element (and indeed has not been). These points have been completely ignored in the examiner's response to Appellant's arguments on pages 12-15 of the Office Action, which instead offers a rebuttal of a tertiary argument Appellant has made (incorporated herein by reference)

the gist of which is that there is no reason to combine Diffie-Hellman with Atjai/Dwork because Diffie-Hellman nowhere mentions lattices, much less using hard lattice problems for any reason. To rebut this, the Examiner embarks on a riff extolling the virtues of Diffie-Hellman.

Appellant will keep its response to the Examiner's observations brief. It doesn't matter how much the Examiner esteems Diffie-Hellman, the point remains that neither relied-upon reference mentions rendering infeasible the possibility of mapping two messages together in the space. For that reason alone, the rejection is legally defective under the MPEP. Moreover, it doesn't matter how much Diffie-Hellman engages in general encryption philosophy or how much of a favorable impression this abstract discussion has had on the examiner, what remains is the fact that nowhere does Diffie-Hellman ever mention lattices or hard lattice problems, much less does Diffie-Hellman suggest that it has any application to hard lattice systems or otherwise motivate the skilled artisan to modify a hard lattice reference, and still much less to do so in the peculiar and highly specific ways proposed throughout the rejection. Nowhere has the Examiner mustered a specific citation to any hard lattice discussion in Diffie-Hellman, because there is none. Throughout the rejections, highly technical and specific parts of Diffie-Hellman which Diffie-Hellman nowhere suggests might apply to hard lattice systems are nevertheless proposed to be dropped wholesale into the hard lattice system of Atjai/Dwork. If ever there was a classic case of impermissible hindsight reconstruction, this is it. The rejections, it is respectfully submitted, stand in need of reversal.

(8c) Argument

In contrast to Claim 1, independent Claim 12 recites in part finding a point "y" of a key lattice $\mathcal{L}$ that is not the same as the auxiliary lattice on which the point x is located, as disclosed in Figure 2 (the

message point x returned by the logic cannot be part of the key lattice). Independent Claim 26 specifies that the message μ or a concatenation thereof is mapped to a message point "x" in n-dimensional space, with the message point "x" being an element of a set of spaced-apart points that are not on the lattice. Both of these modalities for achieving the present advantages have been alleged to be taught in the present inventor's previous publication (Atjai/Dwork), top of page 3. But all this section teaches is that a lattice L can have a dual lattice L*. That's it. No mention subsequently appears to be made of this "dual lattice" L*, much less that a message point "x" is a point of a grid or a point of an auxiliary lattice and that a point "y" is found on a key lattice that is not the same as the auxiliary lattice, as is otherwise recited in Claim 12. This rejection on its face is woefully inadequate to establish a *prima facie* case of obviousness under the law, and consequently is ripe for reversal.

The only remaining allegations to address are those directed against Claim 26, relying of Atjai/Dwork, page 1, bottom of page continuing to page 2; page 2, bottom of page; page 4, second paragraph; and page 14, steps 3-5.

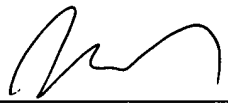
Page 1, bottom continuing to page 2 discusses hyperplanes. The bottom of page 2 contains a definition of a lattice. The second paragraph of page 4 states that the public key can be a random basis the length of which is greater than a parameter by a polynomial factor. Steps 3-5 of page 14 state that a vector is chosen of a length in a predetermined range, and that a private key can be any basis of a particular subspace.

In none of these sections is mapping even discussed, much less mapping a message or a concatenation thereof to a message point "x" in n-dimensional space, with the message point "x" being an element of a set of spaced-apart points not on the lattice. And still further, where in the relied-upon sections is it taught to

find a lattice point "y" of a lattice using the short basis in the context of untaught mapping and unsuggested set of spaced-apart points not on the lattice? The answer, but not the present claims, is obvious: the present invention simply does not exist - not even close - in the relied-upon references as alleged.

The argument in part (8b) above regarding the impropriety of combining the references when there is no prior art teaching to mix apples and oranges as proposed is incorporated in this section (8c).

Respectfully submitted,



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

APPENDIX A - APPEALED CLAIMS

1. A computer-implemented method for digitally signing data, comprising:

generating a lattice $\mathcal{L}$ having at least one short basis establishing a private key and at least one long basis establishing a public key;

mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space using a function "f" rendering infeasible the possibility of mapping two messages together in the space; and

using the short basis, finding a lattice point "y" of the lattice $\mathcal{L}$ that is close to the message point "x".

2. The method of Claim 1, further comprising returning at least the message point "x" and the lattice point "y" as a digital signature.

3. The method of Claim 2, further comprising randomizing the function "f".

4. The method of Claim 3, wherein the function "f" is randomized by concatenating the message μ with a random number ρ.

5. The method of Claim 1, wherein the function "f" maps the message μ to a point on a grid.

6. The method of Claim 5, wherein the function "f" is collision intractable.

7. The method of Claim 6, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

8. The method of Claim 5, wherein the function "f" is not collision intractable.

9. The method of Claim 1, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

10. The method of Claim 1, further comprising verifying a digital signature at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance.

11. The method of Claim 10, wherein the predetermined distance is related to the number of dimensions in the lattice $\mathcal{L}$.

12. A computer program storage device including a program of instructions for generating a digital signature for a message, the program of instructions including:

computer readable code means for mapping a message μ or a concatenation thereof to a message point "x" in n-dimensional space, the message point "x" being a point of a grid or a point of an auxiliary lattice;

computer readable code means for finding a point "y" of a key lattice $\mathcal{L}$ that is not the same as the auxiliary lattice; and

computer readable code means for establishing a digital signature, based at least on the points "x" and "y".

13. The computer program storage device of Claim 12, wherein the means for mapping uses a function "f" rendering infeasible the possibility of mapping two messages close together in the space, and wherein the means for finding includes using a hard to find short basis of the key lattice $\mathcal{L}$.

14. The computer program storage device of Claim 13, further comprising means for randomizing the function "f".

15. The computer program storage device of Claim 14, wherein the function "f" is randomized by concatenating the message μ with a random number ρ.

16. The computer program storage device of Claim 12, wherein the function "f" maps the message μ to a point on a grid, and wherein the function "f" is collision intractable, the collision intractability being derived from the hardness of lattice problems.

17. The computer program storage device of Claim 12, wherein the function "f" is not collision intractable.

18. The computer program storage device of Claim 13, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

19. A computer system for generating a digital signature of a message μ, comprising:

at least one sender computer including logic for executing method steps including:

mapping the message μ to a message point "x" at which it is not feasible to map any other message;

finding a lattice point "y"; and

transmitting at least the message μ and the points "x" and "y";

at least one receiver computer receiving the message μ and points "x" and "y" and including logic for executing method steps including:

determining whether a distance between the points "x" and "y" is related in a predetermined way to a predetermined distance, and based thereon determining whether the message μ has been properly signed.

20. The system of Claim 19, wherein the mapping act is undertaken using a function "f" that maps the message point "x" to a point of a grid or of an auxiliary lattice, and further wherein the lattice point "y" is a member of a lattice $\mathcal{L}$, and the finding act is undertaken using a hard-to-find short basis of the lattice $\mathcal{L}$.

21. The system of Claim 20, wherein the acts undertaken by the logic of the sender computer further comprise randomizing the function "f" by concatenating the message μ with a random number ρ.

22. The system of Claim 20, wherein the function "f" is collision intractable.

23. The system of Claim 22, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

24. The system of Claim 20, wherein the function "f" is not collision intractable.

25. The system of Claim 20, wherein the predetermined distance is related to the number "r" of dimensions in the lattice $\mathcal{L}$.

26. A computer-implemented method for digitally signing data, comprising:

generating a lattice $\mathcal{L}$ having at least one short basis and at least one long basis;

mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space, the message point "x" being an element of a set of spaced-apart points not on the lattice; and

using the short basis, finding a lattice point "y" of the lattice $\mathcal{L}$.

27. The method of Claim 26, wherein the mapping is undertaken using a function "f".

28. The method of Claim 27, further comprising randomizing the function "f" by concatenating the message μ with a random number ρ.

29. The method of Claim 27, wherein the function "f" maps the message μ to a point on a grid.

30. The method of Claim 29, wherein the function "f" is collision intractable.

31. The method of Claim 30, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

32. The method of Claim 29, wherein the function "f" is not collision intractable.

33. The method of Claim 27, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

34. The method of Claim 26, further comprising verifying a digital signature at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance.

35. The method of Claim 34, wherein the predetermined distance is related to the number of dimensions in the lattice $\mathcal{L}$.